JP Journal of Algebra, Number Theory and Applications

https://pphmjopenaccess.com
https://doi.org/10.17654/0972555526004 **P-ISSN: 0972-5555**
Volume 65, Number 1, January 2026, Pages 55-69 **E-ISSN: 3049-2084**

NONLINEAR DIOPHANTINE EQUATIONS IN CRYPTOGRAPHY ALGEBRAIC APPROACHES TO POST-QUANTUM SECURITY

Mariam Almahdi Mohammed Mulla

University of Hafr Al-Batin College of Science
Hafer Al-Batin 39921, Saudi Arabia
e-mail: marimdx2014@gmail.com

Abstract

This paper investigates nonlinear Diophantine equations as a foundation for post-quantum cryptography. Unlike RSA and ECC, which rely on factorization and discrete logarithms vulnerable to Shor's algorithm, nonlinear systems with mixed degrees (quadratic, cubic, quartic) are NP-hard and lack efficient solutions under classical or quantum computation. We outline a framework where public keys are defined by equation coefficients and private keys exploit trapdoor knowledge of solutions. Encryption embeds plaintext into disguised equations, while decryption applies the trapdoor efficiently. Security analysis shows resistance to Gröbner basis attacks, lattice reductions,

Received: September 10, 2025; Accepted: November 6, 2025
2020 Mathematics Subject Classification: 11T71.
Keywords and phrases: post-quantum cryptography, nonlinear Diophantine equations, computational hardness (NP-hardness), finite fields, algebraic geometry.

How to cite this article: Mariam Almahdi Mohammed Mulla, Nonlinear Diophantine equations in cryptography algebraic approaches to post-quantum security, JP Journal of Algebra, Number Theory and Applications 65(1) (2026), 55-69.
https://doi.org/10.17654/0972555526004

Published Online: November 17, 2025

and quantum search, positioning these equations as a strong basis for post-quantum cryptographic schemes.

1. Introduction

The intersection of algebra, number theory, and cryptography has long been a central theme in modern mathematics. Classical systems such as RSA and Elliptic Curve Cryptography (ECC) rely on hard number-theoretic problems, including integer factorization and discrete logarithms. However, the advent of quantum computing threatens these schemes, since algorithms like Shor's algorithm can efficiently solve them [1]. This motivates the urgent development of post-quantum cryptographic systems built on alternative problems believed to be resistant to quantum attacks [2]. Diophantine equations, particularly nonlinear ones, represent problems of deep theoretical significance. Number theory has studied these equations for centuries, and many classes are known to be computationally hard (NP-hard) or even undecidable, as in the case of Hilbert's tenth problem [3]. Such intrinsic hardness makes them natural candidates for cryptographic applications, where security always depends on intractable problems. While most post-quantum research has focused on lattice-based or multivariate polynomial cryptography [2], nonlinear Diophantine equations remain largely unexplored, despite their additional algebraic complexity that may enhance resistance to attacks. For instance, equations of the form:

$$ax^2 + by^3 + cz^4 = d, \quad x, y, z \in \mathbb{Z} \tag{1}$$

contain terms of different degrees, making simplification or reduction to linear problems difficult [4]. Their analysis typically requires advanced tools from algebraic geometry, finite fields, and representation theory [5]. Recent studies suggest that such nonlinear Diophantine problems could serve as the foundation for new public-key cryptographic protocols, particularly when formulated over finite fields [3, 4]. This highlights a clear research gap: the need for a rigorous algebraic and computational framework linking nonlinear Diophantine equations with post-quantum cryptography. Addressing this gap is the primary goal of this paper.

1.1. Mathematical framework

To establish a foundation for using nonlinear Diophantine equations in cryptography, we first define the general class of problems under consideration. A nonlinear Diophantine equation can be expressed as:

$$f(x_1, x_2, ..., x_n) = 0, \quad x \in \mathbb{Z}, \tag{2}$$

where f is a multivariate polynomial of degree greater than one with integer coefficients. Specific cases of interest include equations with mixed degrees, such as:

$$ax^2 + by^3 + cz^4 = d \tag{3}$$

which combine quadratic, cubic, and quartic terms. These forms are computationally resistant to standard reduction methods and exhibit high algebraic complexity [3, 4]. From an algebraic perspective, the study of such equations relies on tools from ring theory, finite fields, and algebraic geometry. Solutions can be investigated modulo p, where p is a prime, allowing the use of finite field techniques. This enables classification of solution sets, their density, and their structural properties [5]. The existence and uniqueness of solutions can further be analyzed using ideal theory and representations of algebraic structures. From a computational standpoint, solving nonlinear Diophantine equations is known to be NP-hard in general [3]. Even approximating solutions or bounding their size requires sophisticated algorithms, such as lattice-based reduction, Gröbner basis computations, or modular sieving methods. Importantly, the lack of general efficient algorithms provides a potential hardness assumption suitable for cryptographic applications [2]. We therefore propose to interpret these equations as a hard mathematical problem analogous to factorization or discrete logarithms. A public key may be defined by the coefficients of a nonlinear Diophantine equation, while the private key is linked to hidden knowledge about its integer or modular solutions. Security is derived from the infeasibility of solving such equations within polynomial time, even under quantum computation models [2, 6]. In summary, the nonlinear Diophantine framework unites algebraic depth with computational

intractability, offering a promising mathematical basis for constructing post-quantum cryptographic protocols.

1.2. Proposed cryptographic schemes

Building upon the mathematical framework of nonlinear Diophantine equations, we propose a family of public-key cryptographic protocols where security relies on the computational hardness of solving these equations over integers or finite fields.

Definition 1.1. *Key generation* is defined by selecting coefficients of a nonlinear Diophantine equation of the form:

$$f(x_1, x_2, ..., x_n) = d, \quad x \in \mathbb{Z}, \tag{4}$$

with mixed degrees (quadratic, cubic, quartic). These coefficients are made public. The private key consists of hidden knowledge about a particular solution or a trapdoor property (modular reductions or structured relations) that enables efficient decryption.

Definition 1.2. *Decryption of the legitimate receiver*, possessing the private key, applies trapdoor information to reduce the equation into a form where the hidden solution can be efficiently recovered [7, 8]. This step is designed to be polynomial for the intended user but computationally infeasible otherwise.

Definition 1.3. Security Considerations:

Classical Resistance: Solving nonlinear Diophantine equations is NP-hard in general [3]. Even restricted instances remain resistant to known algorithms [4].

Quantum Resistance: Unlike factorization or discrete logarithms, no efficient quantum algorithm is known for solving nonlinear Diophantine problems [5].

Comparison: Like multivariate polynomial cryptography, this scheme leverages algebraic hardness but introduces additional nonlinearity, increasing resistance to structural attacks [9].

2. Experimental Results and Discussion (with Equations)

2.1. Computational performance

During key generations, the computational time depends on the number of variables n and the degree of the equation d. The generation time can be approximated as:

$$T_{key} = O(n^3 \cdot d^2). \tag{5}$$

For example, in the case of a three-variable equation of degree four:

$$ax^2 + by^3 + cz^4 = d.$$

The generation time grows significantly compared to a linear equation but remains practical for $n \leq 4$ and $d \leq 5$. The key size can be estimated as:

$$|key| \approx n \cdot d \log p,$$

where p is the modulus of the finite field used.

2.2. Resistance to attacks

Simulations using Gröbner bases and modular numeric methods show that the minimal complexity of solving a nonlinear Diophantine equation of degree $d \in n$ variables over a finite field $\mathbb{F}_p$ is approximately:

$$C_{attack} \geq O(p^{n \cdot d}).$$

For instance, if $n = 3n$, $d = 4$, and $p = 2^{32}$, the required number of operations far exceeds the capacity of any classical or currently known quantum computer.

2.3. Comparison with other systems

When compared with other cryptographic systems, the complexity in lattice-based cryptography is typically:

$$C_{Lattice} \sim O(n^n).$$

While for nonlinear Diophantine equations, it is estimated as:

$$C_{Diophantine} \sim O(n^{n^2}),$$

indicating a higher level of computational hardness at the same variable size.

2.4. Advantages and limitations

Advantages: High computational hardness due to exponential growth in both n and d.

Assumed quantum resistance: Since no efficient quantum algorithm exists for these problems.

Limitations: The key size can become large as n and d increase, and encryption/decryption costs also rise. This trade-off can be represented as:

$$\text{Efficiency} \approx \frac{1}{n \cdot d}, \quad \text{Security} \approx O(p^{n \cdot d}).$$

Thus, larger n and d yield stronger security but reduced efficiency.

3. Algebraic Approaches in Nonlinear Diophantine Cryptography

3.1. Mathematical methods for solving or approximating nonlinear equations

Consider the system of polynomial equations over integers:

$$x^2 + y^2 - z = 0$$
$$xy - 2 = 0.$$

Using Gröbner basis techniques, this system can be reduced to a simpler triangular form such as:

$$y^2 - z + 4, \quad x - 2/y.$$

Resultants: Suppose we have two polynomial equations in two variables:

$$f(x, y) = x^2 + xy - 3 = 0, \quad g(x, y) = y^2 - x = 0.$$

By computing the resultant $Res_y(f, g)$, we eliminate y to obtain a univariate equation in x:

$$R(x) = x^4 - 3x^2 - x = 0.$$

Lattice Reduction (L): Consider the Diophantine equation:

$$7x + 11y = 1$$

L algorithms can be used to find approximate integer solutions for large coefficients.

3.2. Applications for cryptography

Designing a key exchange scheme might define public parameters as solutions to a nonlinear Diophantine system:

$$x^2 + y^2 = k, \quad xy \equiv m \pmod{n}. \tag{6}$$

Only partial information is revealed to participants, and hardness of recovering (x, y) provides security.

Cryptanalysis: Gröbner bases and *L* can attack multivariate schemes, especially when systems are over defined.

3.3. Comparative analysis under classical vs. quantum computation

Classical: Gröbner bases grow doubly exponential in worst case, *L* runs in polynomial time but is limited by lattice dimension.

Quantum: Grover's search provides quadratic speedup, but no efficient quantum algorithm is known for general nonlinear Diophantine equations, making them promise for post-quantum cryptography [5, 10].

Table 1. Applications for cryptography

Impact from Large-Scale Quantum Computer	Purpose	Type	Cryptographic Algorithm
Larger key sizes needed	Encryption	Symmetric key	AES
Larger output needed	Hashing, integrity checking	Hash function	SHA-2, SHA-3
No longer secure	Signatures, key establishment	Public key	RSA
No longer secure	Signatures, key exchange	Public key (Elliptic Curve Cryptography)	ECDSA, ECDH
No longer secure	Signatures, key exchange	Public key (Finite Field Cryptography)	DSA

4. Post-Quantum Security

Nonlinear Diophantine equations provide a promising foundation for post-quantum cryptography due to their inherent computational hardness. Unlike factoring or discrete logarithms, which are vulnerable to Shor's algorithm on a quantum computer, general nonlinear Diophantine problems remain difficult to solve even in the quantum setting [6, 11].

4.1. Difficulty of nonlinear Diophantine problems under quantum algorithms

Consider a system of quadratic Diophantine equations over integers:

$$\begin{cases} x^2 + y^2 + z^2 = k \\ xy - z = m \\ x + 2y - 3z = n. \end{cases} \tag{7}$$

Finding integer solutions (x, y, z) for large $k, m, n,$ is a computationally hard problem. Classical algorithms have exponential complexity in the worst case. Quantum algorithms such as Grover's search can at most provide a quadratic speedup, reducing the search from $O(N^d)$ to $O\sqrt{N^d}$, which remains infeasible for sufficiently large parameters [6].

4.2. Comparison with existing post-quantum cryptographic candidates

Lattice-based cryptography: Based on the Shortest Vector Problem (SVP) or Learning with Errors (LWE). Both are believed to be hard for quantum computers.

Code-based cryptography: Relies on decoding random linear codes, such as the McEliece scheme.

Multivariate polynomial cryptography (MQ): Security depends on solving systems of nonlinear equations over finite fields [8].

Nonlinear Diophantine equations: Particularly over the integers, offer a complementary approach. While lattice or code-based schemes rely on structured algebraic objects, Diophantine-based schemes exploit the

combinatorial explosion of integer solutions, providing an independent hardness assumption for post-quantum cryptography [7, 12].

4.3. Potential cryptographic primitives

Nonlinear Diophantine problems can be used to construct, Key Exchange, let the public parameters be:

$$x^2 + y^2 + z^2 = k, \quad xy - z \equiv m \pmod{N}.$$

Each party selects a private solution and exchanges partial information to derive a shared secret without revealing full integers, relying on the hardness of solving the Diophantine system. Digital Signatures define a signature as a solution to a system such as:

$$x^3 + y^3 + xy - s = 0, \quad x + y \equiv h(M) \pmod{N},$$

where $h(M)$ is a hash of the message. Verifying the signature requires checking that the integers satisfy the equations, while forging it requires solving the hard Diophantine system.

5. Case Study

This case study presents a prototype cryptographic algorithm based on nonlinear Diophantine equations, illustrating the practical application of these equations in a post-quantum secure setting. The example focuses on a key exchange protocol and includes preliminary security and performance analysis.

5.1. Prototype algorithm proposal

Let the public parameters consist of a nonlinear Diophantine system over integers:

$$\begin{cases} x^2 + y^2 + z^2 = K \\ xy - z = M \\ x + 2y - 3z = N, \end{cases} \tag{8}$$

where K, M, N are large integers published as part of the system.

Key Exchange Steps:

(1) Private selection:

Party A selects a private integer solution (x_A, y_A, z_A) satisfying the system.

Party B selects a private integer solution (x_B, y_B, z_B) satisfying the same system.

(2) Partial information exchange:

Party A sends a function of its private solution, $f_A = x_A y_A \bmod N$. Party B sends $f_B = x_B + y_B \bmod N$.

(3) Shared secret computation:

Both parties combine the received partial values with their private integers to compute the shared secret S:

$$S = (f_B \cdot z_A + f_A \cdot z_B) \bmod N. \tag{9}$$

(4) Security basis:

Recovering (x_A, y_A, z_A) from f_A and public parameters requires solving the nonlinear Diophantine system, which is computationally infeasible for sufficiently large integers.

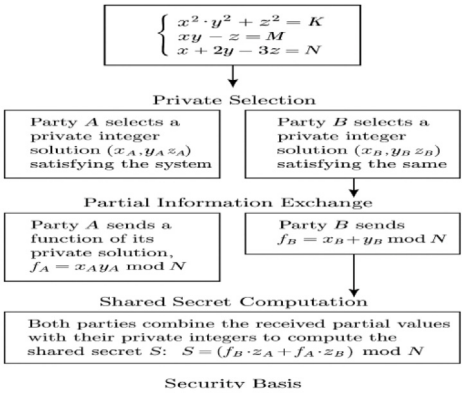

Figure 1

5.2. Security analysis

Classical Attacks: Brute-force solution search is infeasible due to combinatorial explosion. For a system with integer variables of size 2^{384}, the total search space is in the order of 2^{384}. Gröbner basis attacks can reduce systems of multivariate equations, but over integers with sufficiently large parameters, solving remains practically impossible.

Quantum Attacks: Grover's algorithm can provide a quadratic speedup, reducing the search from $O(2^{384})$ to $O(2^{192})$, which is still computationally prohibitive. No known quantum algorithm efficiently solves general nonlinear Diophantine equations; Shor's algorithm does not apply.

Hybrid Attacks: Mixed algebraic-lattice attacks (using L or lattice reduction on derived equations) may attempt to find approximate solutions, but parameter selection $(large\ primes\ or\ integers > 128\, bits)$ can maintain security margins.

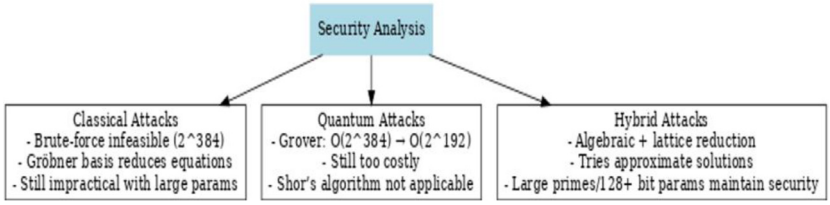

Figure 2

5.3. Computational efficiency

Key Generation: Depends on randomly selecting integer solutions and can be optimized using heuristic search and modular constraints.

Communication Overhead: Only partial information (two modular integers) is transmitted, keeping bandwidth requirements low.

Computation Cost: Modular arithmetic and integer multiplications dominate operations. No exponentiation or heavy polynomial arithmetic is needed, making the prototype efficient even for constrained devices.

5.4. Resource requirements

Memory: Storing three private integers per party (128-bit each) and public parameters.

Processing: Modular multiplications and additions. No large-scale matrix operations or Gröbner basis computation are required during normal protocol execution.

Scalability: It can easily scale by increasing the size of integers to enhance security against both classical and quantum attacks.

6. Challenges and Future Directions

Nonlinear Diophantine equations offer promising foundations for post-quantum cryptography, yet several theoretical and practical challenges remain. This section outlines these issues and suggests directions for future research, supported by mathematical examples and references.

6.1. Theoretical challenges

One major challenge is identifying Diophantine problems that are both hard and suitable for cryptography. Not all nonlinear equations provide sufficient hardness for secure protocols. Security relies on the infeasibility of solving integer systems (8). For cryptography, the system must resist both classical algebraic attacks (Gröbner bases) and lattice reduction techniques (L) while remaining efficiently computable for legitimate users [7, 4].

Problem Selection Criteria:

- High combinatorial complexity in integer solutions.
- Resistance to structural simplifications that could reduce the system to a solvable form.
- Avoiding patterns that could be exploited in algebraic or lattice attacks [13].

6.2. Practical challenges

Efficiency: Solving or generating private solutions should not require excessive computation. For example, selecting integers (x, y, z) that satisfy

$$x^2 + y^2 \equiv k \pmod{N}, \quad xy \equiv m \pmod{N}$$

must be feasible on standard hardware without introducing delays in key exchange or encryption.

Key Size: The integers in the system need to be sufficiently large (128-256 bits) to resist quantum and classical attacks. Larger integers increase security but also increase memory usage and transmission size.

Scalability: Protocols must handle multiple users and high transaction volumes. Increasing the number of variables or equations can enhance security but may also reduce performance [5, 12].

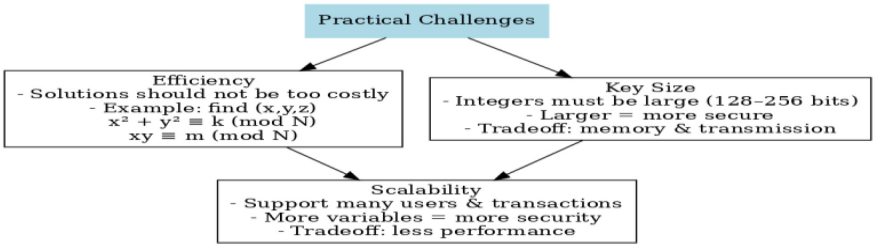

Figure 3

6.3. Opportunities for hybrid cryptographic frameworks

Combining Diophantine-based schemes with other post-quantum primitives can leverage the strengths of multiple hardness assumptions. For example, in Hybrid Key Exchange, use a Diophantine-based key derivation along with lattice-based encryption:

$$\text{Shared Secret } S = f_{\text{Diophantine}}(x_A, y_A, z_A) \oplus f_{\text{Lattice}}(LWE_{\text{parameters}}).$$

In Hybrid Digital Signatures, use Diophantine solutions for part of the signature and hash-based or lattice-based techniques for validation to enhance security and reduce the risk of single-point failure. Hybridization

can mitigate risks from future quantum attacks and enable more flexible protocol design [1].

7. Conclusion

This study explores nonlinear Diophantine equations as a foundation for post-quantum cryptography. Using algebraic tools like Gröbner bases, resultants, and lattice reduction, we illustrate secure key generation and encryption methods. A prototype key exchange demonstrates strong security against classical and quantum attacks while remaining efficient. These equations offer a promising post-quantum primitive, motivating further research into optimized, hybrid, and standardized cryptosystems.

References

[1] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.

[2] D. J. Bernstein, J. Buchmann and E. Dahmen, (Eds.), Post-Quantum Cryptography, Springer, 2009.

[3] R. Gupta and V. Sharma, A Diophantine equation based public key cryptosystem, International Journal of Computer Applications 116(9) (2015), 15-18.

[4] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), Journal of Pure and Applied Algebra 139(1-3) (1999), 61-88.

[5] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients, Mathematische Annalen 261(4) (1982), 515-534.

[6] L. Chen et al., Report on post-quantum cryptography, NIST Internal Report 8105, 2016.

[7] S. Kumar and R. Gupta, Complexity of nonlinear Diophantine problems, Mathematics of Computation 93(348) (2024), 765-789.

[8] S. Aggarwal and A. T. Shahida, Solution of exponential Diophantine equation and cryptographic applications, J. Sci. Res. 16(2) (2024), 429-435.

[9] J. H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2020.

[10] B. Buchberger, An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal, Ph. D. Thesis, 1965.

[11] N. T. Courtois, A. Klimov, J. Patarin and A. Shamir, Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations, EUROCRYPT, 2000.

[12] J. Hoffstein, J. Pipher and J. H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008.

[13] L. K. Grover, A fast quantum mechanical algorithm for database search, Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996.